

Department of the Interior
Privacy Impact Assessment

Name of Project: Performance Management Database System (PMDS)

Bureau: National Park Service

Project's Unique ID: DOI_NPS_167

A. CONTACT INFORMATION:

1) Who is the Bureau/Office Privacy Act Officer who reviewed this document?

Felix Uribe
NPS Privacy Officer
(202) 357-6925

B. SYSTEM APPLICATION/GENERAL INFORMATION:

- 1) Does this system contain any information about individuals?** Yes, it contains NPS email addresses and telephone numbers.

a. Is this information identifiable to the individual¹¹? Yes.

(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

b. Is the information about individual members of the public? No.

(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

c. Is the information about employees? Yes.

(If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

- 2) What is the purpose of the system/application?** The Performance Management Data System (PMDS) is a web-enabled application designed to support the Government Performance Reporting Act (GPRA). It is used to plan, track, and report performance against goals and aggregate totals to the Park, Region, and National levels.

- 3) What legal authority authorizes the purchase or development of this system/application?** Directors Orders #54 - Management Accountability

C. DATA in the SYSTEM:

- 1) What categories of individuals are covered in the system?** Federal Employees of the National Park Service who are acting as Government Performance Reporting Act (GPRA) Coordinators.

¹¹ "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

2) What are the sources of the information in the system?

- a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?** The individual provides the information.
- b. What Federal agencies are providing data for use in the system?** The National Park Service.
- c. What Tribal, State and local agencies are providing data for use in the system?** None.
- d. From what other third party sources will data be collected?** None.
- e. What information will be collected from the employee and the public?** Last Name, First Name, NPS email address and telephone number.

3) Accuracy, Timeliness, and Reliability

- a. How will data collected from sources other than DOI records be verified for accuracy?** Not applicable.
- b. How will data be checked for completeness?** PMDS validates data, user denied access if validation fails.
- c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).** Periodically, users are prompted to verify their data before accessing the system.
- d. Are the data elements described in detail and documented? If yes, what is the name of the document?** The data elements are described in detail on the screen and in the PMDS documentation.

D. ATTRIBUTES OF THE DATA:

- 1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?** Yes.
- 2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?** No.
- 3) **Will the new data be placed in the individual's record?** No. It is maintained separately in the database as part of the users PMDS account.
- 4) **Can the system make determinations about employees/public that would not be possible without the new data?** No. The same data contained within - the system is also freely available to the public at www.nps.gov.
- 5) **How will the new data be verified for relevance and accuracy?** Periodically, users are prompted to verify their data before accessing the system.
- 6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?** Only PMDS system administrators have access to this data. User account level security and table/row level security is in place in the Oracle 10g database, as well as NPS firewall and active directory security procedures. Data is not being aggregated.
- 7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.** Only PMDS system administrators have access to this data. User account level security and table/row level security is in place in the Oracle 10g database, as well as NPS firewall and active directory security procedures. Processes are not being consolidated.
- 8) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.** The individual's User ID provides access to that individuals data only.

- 9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?** There are no reports containing this data.
- 10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)** Individuals must provide this information.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

- 1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?** Data is maintained at one secure location at the NPS Eye Street Data Center, Washington, D.C..
- 2) **What are the retention periods of data in this system?** Data is retained until the user account is deactivated.
- 3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?** Data is maintained indefinitely, until the user account is deactivated.
- 4) **Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?** No.
- 5) **How does the use of this technology affect public/employee privacy?** Not applicable.
- 6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.** No.
- 7) **What kinds of information are collected as a function of the monitoring of individuals?** Not applicable.
- 8) **What controls will be used to prevent unauthorized monitoring?** Not applicable.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name. Federal Financial System- Interior, DOI - 90

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain. No. System is not being modified.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other) Users (each user has access to only their own data), system administrators, system manager.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Access is determined by User ID and system security role. These roles are documented. Among all user roles except system administrator, users have access to only their own data.

3) Will users have access to all data on the system or will the user's access be restricted? Explain. System access is restricted according to User ID and system security role. Among all user roles, except system administrator, users have access to only their own data.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials) System access controls are in place, and among all users except system administrators, users have access to only their own data. In addition, user's roles and access is covered in the PMOS User's Guide.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Yes, a contractor was involved in the development of the system and Privacy Act clauses were in the contract and annual training was mandatory during that period of time. At the present time all, maintenance is being performed by NPS employees only.

6) Do other systems share data or have access to the data in the system? If yes, explain. No other systems have access to user account data.

- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?** NPS Office of the Comptroller.
- 8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?** No.
- 9) How will the data be used by the other agency?** Not applicable.
- 10) Who is responsible for assuring proper use of the data?** NPS Office of the Comptroller.